





# Encriptado por hardware Vs software

Comprender las diferencias clave y cuál es la mejor opción para sus necesidades.



En la lucha constante por la seguridad de los datos, la diferencia entre el encriptado por hardware y el encriptado por software se reduce a dónde reside la seguridad y cuán expuesta está en la práctica. En las unidades USB y SSD, el lugar donde se crea el encriptado determina el nivel de seguridad con el que se protegen los datos y en qué medida depende del sistema que lo rodea.

| HARDWARE  | VS | SOFTWARE   |
|---|----|--|
|  <p><b>Manejo de claves de encriptación</b><br/>Las claves de encriptado son generadas internamente por el hardware y almacenadas de forma segura dentro de la unidad.</p>   |    |  <p><b>Manejo de claves de encriptación</b><br/>La contraseña del usuario se utiliza directamente como la clave de encriptado, y las claves pueden residir en la memoria del sistema.</p>   |
|  <p><b>Protección contra ataques de fuerza bruta</b><br/>Diseñadas para proteger contra ataques de fuerza bruta al limitar el número de intentos antes de que la unidad se borre a sí misma evitando que cualquier persona acceda a los datos confidenciales en caso de pérdida o robo de la unidad.</p> |    |  <p><b>Protección contra ataques de fuerza bruta</b><br/>Sensible a los ataques de fuerza bruta, la computadora intenta limitar el número de intentos de descifrado, pero los piratas informáticos pueden acceder a la memoria de la computadora y restablecer el contador de intentos.</p> |
|  <p><b>Se requiere software o controlador</b><br/>No requiere instalación de controladores o software en el sistema huésped.</p>   |    |  <p><b>Se requiere software o controlador</b><br/>Requiere instalación de software, los controladores y la compatibilidad del sistema operativo pueden variar.</p>  |
|  <p><b>Recursos de encriptación</b><br/>Utiliza un procesador criptográfico especializado integrado en la propia unidad.</p>   |    |  <p><b>Recursos de encriptación</b><br/>Utiliza la CPU de la computadora huésped y los recursos del sistema para cifrar y descifrar datos.</p>  |
|  <p><b>Dependencia / exposición del sistema huésped</b><br/>La seguridad está aislada dentro del dispositivo y permanece protegida incluso cuando está conectada a computadoras no confiables o infectadas.</p>  |    |  <p><b>Dependencia / exposición del sistema huésped</b><br/>La seguridad depende del sistema operativo del huésped y es más vulnerable si el equipo está infectado con malware.</p>   |
|  <p><b>Estado de encriptación</b><br/>El encriptado está siempre activado por diseño y no se puede eliminar ni omitir.</p>   |    |  <p><b>Estado de encriptación</b><br/>El encriptado puede estar habilitado, deshabilitado o mal configurado.</p>  |
|  <p><b>Impacto en el rendimiento</b><br/>Impacto mínimo en el rendimiento, ya que el encriptado se descarga en el procesador de hardware.</p>  |    |  <p><b>Impacto en el rendimiento</b><br/>Puede afectar negativamente al rendimiento porque el encriptado comparte recursos de la CPU.</p>   |
|  <p><b>Flexibilidad</b><br/>El encriptado está vinculado a la unidad USB o SSD específica.</p>   |    |  <p><b>Flexibilidad</b><br/>Se puede utilizar en casi cualquier medio de almacenamiento.</p>  |



El encriptado por software ofrece flexibilidad, mientras que el encriptado por hardware mantiene la seguridad aislada y menos expuesta a los riesgos a nivel del sistema. Comprender cómo cada uno protege los datos y controla el acceso, lo ayuda a elegir el nivel de seguridad adecuado para sus flujos de trabajo y perfil de riesgo.